CLAIMS

What is claimed is:

_	_			
1		An apparatus com	nricinc	٠,
1	1.	An apparatus com	(DIIOIII)	٤.

- a modular multiplier including a plurality of independent computation channels, said plurality of independent computation channels including a first computation channel and a second computation channel;
- a coupling device interposed between said first computation channel and said second computation channel to receive a first control signal and to couple said first computation channel to said second computation channel in response to a receipt of said first control signal.
- 1 2. The apparatus as set forth in claim 1, wherein said modular multiplier comprises
- 2 a linear systolic array of processing elements, said linear systolic array of processing
- 3 elements including said plurality of independent computation channels.
- 1 3. The apparatus as set forth in claim 1, wherein said coupling device comprises a
- 2 coupling device to receive a second control signal and to selectively couple said first
- 3 computation channel to said second computation channel in response to a state of said
- 4 second control signal.
- 1 4. The apparatus as set forth in claim 3, said apparatus having a first mode of
- 2 operation corresponding to a first state of said second control signal wherein said first
- 3 computation channel is operably separated from said second computation channel and a
- 4 second mode of operation corresponding to a second state of said second control signal
- 5 wherein said first computation channel is operably coupled to said second computation
- 6 channel via said coupling device.
- 1 5. The apparatus as set forth in claim 4, wherein said first computation channel and
- 2 said second computation channel operate as two n-bit modular multipliers in said first
- 3 mode of operation and as a single 2n-bit modular multiplier in said second mode of
- 4 operation, where n is an integer.

- 1 6. The apparatus as set forth in claim 5, where n is 512.
- 1 7. The apparatus as set forth in claim 1, wherein said modular multiplier comprises
- 2 a Montgomery multiplier.
- 1 8. The apparatus as set forth in claim 1, wherein said a coupling device comprises a
- 2 first multiplexer coupled between an output of said first computation channel and an
- 3 input of said second computation channel and a second multiplexer coupled between an
- 4 output of said second computation channel and an input of said first computation
- 5 channel.

1

7

- 9. A processor comprising:
- a modular multiplier including a plurality of independent computation channels.
- 3 said plurality of independent computation channels including a first computation channel
- 4 and a second computation channel;
- 5 a coupling device interposed between said first computation channel and said
- 6 second computation channel to receive a first control signal and to couple said first
 - computation channel to said second computation channel in response to a receipt of said
- 8 first control signal.
- 1 10. The processor as set forth in claim 9, wherein said modular multiplier comprises
- 2 a linear systolic array of processing elements, said linear systolic array of processing
- 3 elements including said plurality of independent computation channels.
- 1 11. The processor as set forth in claim 9, wherein said coupling device comprises a
- 2 coupling device to receive a second control signal and to selectively couple said first
- 3 computation channel to said second computation channel in response to a state of said
- 4 second control signal.
- 1 12. The processor as set forth in claim 11, said processor having a first mode of
- 2 operation corresponding to a first state of said second control signal wherein said first
- 3 computation channel is operably separated from said second computation channel and a

- 4 second mode of operation corresponding to a second state of said second control signal
- 5 wherein said first computation channel is operably coupled to said second computation
- 6 channel via said coupling device.
- 1 13. The processor as set forth in claim 12, wherein said first computation channel and
- 2 said second computation channel operate as two n-bit modular multipliers in said first
- 3 mode of operation and as a single 2n-bit modular multiplier in said second mode of
- 4 operation, where n is an integer.
- 1 14. The processor as set forth in claim 13, where n is 512.
- 1 15. The processor as set forth in claim 9, wherein said modular multiplier comprises
- 2 a Montgomery multiplier.
- 1 16. The processor as set forth in claim 9, wherein said a coupling device comprises a
- 2 first multiplexer coupled between an output of said first computation channel and an
- 3 input of said second computation channel and a second multiplexer coupled between an
- 4 output of said second computation channel and an input of said first computation
- 5 channel.
- 1 17. A system comprising:
- a memory to store data and instructions;
- a first processor coupled to said memory to process data and execute instructions;
- 4 and
- 5 a second processor coupled to said memory, said second processor comprising:
- a modular multiplier including a plurality of independent computation
- 7 channels, said plurality of independent computation channels including a first
- 8 computation channel and a second computation channel;
- 9 a coupling device interposed between said first computation channel and
- said second computation channel to receive a first control signal and to couple
- 11 said first computation channel to said second computation channel in response to
- 12 a receipt of said first control signal.

- 1 18. The system as set forth in claim 17, wherein said modular multiplier comprises a
- 2 linear systolic array of processing elements, said linear systolic array of processing
- 3 elements including said plurality of independent computation channels.
- 1 19. The system as set forth in claim 17, wherein said coupling device comprises a
- 2 coupling device to receive a second control signal and to selectively couple said first
- 3 computation channel to said second computation channel in response to a state of said
- 4 second control signal.
- 1 20. The system as set forth in claim 19, said second processor having a first mode of
- 2 operation corresponding to a first state of said second control signal wherein said first
- 3 computation channel is operably separated from said second computation channel and a
- 4 second mode of operation corresponding to a second state of said second control signal
- 5 wherein said first computation channel is operably coupled to said second computation
- 6 channel via said coupling device.
- 1 21. The system as set forth in claim 20, wherein said first computation channel and
- 2 said second computation channel operate as two n-bit modular multipliers in said first
- 3 mode of operation and as a single 2n-bit modular multiplier in said second mode of
- 4 operation, where n is an integer.
- 1 22. The system as set forth in claim 17, wherein said a coupling device comprises a
- 2 first multiplexer coupled between an output of said first computation channel and an
- 3 input of said second computation channel and a second multiplexer coupled between an
- 4 output of said second computation channel and an input of said first computation
- 5 channel.

1

- 23. A method comprising:
- 2 receiving a first control signal and a plurality of operands; and
- 3 performing a modular multiplication operation on said plurality of operands
- 4 utilizing a modular multiplier including a plurality of independent computation channels,
- 5 said plurality of independent computation channels including a first computation channel

6	and a second computation channel, wherein performing said modular multiplication		
7	operation comprises:		
8	coupling said first computation channel with said second computation		
9	channel in response to receiving said first control signal;		
10	performing a first portion of said modular multiplication operation		
l 1	utilizing said first computation channel; and		
12	performing a second portion of said modular multiplication operation		
13	utilizing said second computation channel.		
1	24. The method as set forth in claim 23, wherein performing a modular multiplication		
2	operation comprises performing a modular multiplication operation on said plurality of		
3	operands utilizing a modular multiplier including a linear systolic array of processing		
4	elements, said linear systolic array of processing elements including said plurality of		
5	independent computation channels.		
1	25. The method as set forth in claim 23, wherein:		
2	performing a first portion of said modular multiplication operation comprises		
3	providing said plurality of operands to said first computation channel and processing said		
4	plurality of operands utilizing said first computation channel to produce an intermediate		
5	result;		
6	coupling said first computation channel with said second computation channel		
7	comprises providing said intermediate result to said second computation channel; and		
8	performing a second portion of said modular multiplication operation comprises		
9	processing said intermediate result utilizing said second computation channel.		
1	26. The method as set forth in claim 23, said method further comprising receiving a		
2	second control signal, wherein coupling said first computation channel with said second		
3	computation channel comprises selectively coupling said first computation channel with		
4	said second computation channel in response to receiving said second control signal.		
1	27. A machine-readable medium having a plurality of machine-executable		
2	instructions embodied therein which when executed by a machine, cause said machine to		
3	perform a method comprising:		

4	receiving a first control signal and a plurality of operands; and		
5	performing a modular multiplication operation on said plurality of operands		
6	utilizing a modular multiplier including a plurality of independent computation channels,		
7	said plurality of independent computation channels including a first computation channel		
8	and a second computation channel, wherein performing said modular multiplication		
9	operation comprises:		
10	coupling said first computation channel with said second computation		
11	channel in response to receiving said first control signal;		
12	performing a first portion of said modular multiplication operation		
13	utilizing said first computation channel; and		
14	performing a second portion of said modular multiplication operation		
15	utilizing said second computation channel.		
1	28. The machine-readable medium as set forth in claim 27, wherein performing a		
2	modular multiplication operation comprises performing a modular multiplication		
3	operation on said plurality of operands utilizing a modular multiplier including a linear		
4	systolic array of processing elements, said linear systolic array of processing elements		
5	including said plurality of independent computation channels.		
1	29. The machine-readable medium as set forth in claim 27, wherein:		
2	performing a first portion of said modular multiplication operation comprises		
3	providing said plurality of operands to said first computation channel and processing said		
4	plurality of operands utilizing said first computation channel to produce an intermediate		
5	result;		
6	coupling said first computation channel with said second computation channel		
7	comprises providing said intermediate result to said second computation channel; and		
8	performing a second portion of said modular multiplication operation comprises		
9	processing said intermediate result utilizing said second computation channel.		
1	30. The machine-readable medium as set forth in claim 27, said method further		
2	comprising receiving a second control signal, wherein coupling said first computation		
3	channel with said second computation channel comprises selectively coupling said first		

- 4 computation channel with said second computation channel in response to receiving said
- 5 second control signal.